What is claimed is:

sub. a1

1. A method of monitoring the execution of a software component associated with an application in accordance with a predetermined security policy, said method comprising the steps of:

intercepting application programming interface (API) calls issued by the software component;

blocking intercepted API calls that are forbidden according to the security policy; and

allowing intercepted API calls that are permitted according to the security policy.

2. The method according to claim 1, wherein said step of intercepting comprises the steps of:

injecting a security monitor into the address space of the application; and

redirecting said preselected set of API calls issued by the software component to said security monitor.

3. The method according to claim 1, wherein said step of blocking intercepted API calls comprises the step of blocking intercepted API calls that are in the preselected set of APIs.

4. The method according to claim 1, wherein said step of allowing intercepted API calls comprises the step of allowing intercepted API calls that are in the preselected set of APIs.

5. A method of monitoring the execution of a software component associated with an application in accordance with a predetermined security policy, said method comprising the steps of:

intercepting a preselected set of application programming interface (API) calls issued by the application;

intercepting non-API calls issued by the software component;

determining whether an intercepted API call issued by the application originated from a non-API call issued by the software component;

blocking intercepted API calls that originated with a non-API call from the software component that are forbidden according to the security policy; and

31

~~allowing intercepted API calls that originated with a non-API call from the software component that are permitted according to the security policy.~~

~~6. The method according to claim 5, wherein said step of intercepting a preselected set of API calls issued by the application comprises the steps of:~~

~~injecting a security monitor into the address space of the monitored application; and~~

~~redirecting said preselected set of API calls issued by the application to said security monitor.~~

~~7. The method according to claim 5, wherein said step of intercepting non-API calls issued by the software component comprises the steps of:~~

~~injecting a security monitor into the address space of the monitored application; and~~

~~redirecting said non-API calls issued by the software component to said security monitor.~~

~~8. A method of monitoring the execution of a software component associated with an application in accordance with a predetermined security policy, said method comprising the steps of:~~

~~injecting a security monitor into the address space of the application;~~

~~generating a plurality of stub functions corresponding to application programming interface (API) calls and non-API functions which are called by the software component;~~

~~redirecting API calls and non-API calls made by the software component;~~

~~redirecting API calls made by the application to said security monitor;~~

~~setting a flag with each call made by the software component;~~

~~redirecting a portion of API calls received by said plurality of stub functions to said security monitor;~~

~~redirecting said non-API calls made by the software component to their corresponding non-API functions; and~~

~~applying the predetermined security policy to an API call when said flag is set.~~

~~9. A method of monitoring the execution of a software component associated with an application in accordance with a predetermined security policy, said method comprising the steps of:~~

~~applying interception to the application including all its modules whether loaded initially or during execution thereof;~~

~~detecting the loading of a software component external to the application;~~

~~applying interception to all calls made by the software component to functions located in other modules; and~~

~~applying the security policy to said calls made by the software component.~~

~~10. A method of monitoring the execution of a software component associated with an application in accordance with a predetermined security policy, said method comprising the steps of:~~

~~applying interception to the application including all its modules whether loaded initially or during execution thereof;~~

~~detecting the loading of a software component external to the application;~~

~~applying interception to all calls made by the software component to functions located in other modules; and~~

~~setting a flag when a call is issued by the software component to any function located in another module;~~

~~applying interception to API calls contained in a preselected set; and~~

~~applying the security policy to an API call when said flag is set.~~

add a2